5. $\mathbb{N}$ à partir de Peano-Dedekind

Pour la culture générale et la force des idées . . .

1. $\mathbb{N}$ par les axiomes de Peano-Dedekind
2. Sur l'unicité de $\mathbb{N}$
3. Addition dans $\mathbb{N}$
4. Multiplication dans $\mathbb{N}$
5. Structure d'ordre
6. Cardinaux, ensembles finis (et infinis ?)
7. Division euclidienne
8. Nombres premiers selon Euclide

1. $\mathbb{N}$ par les axiomes de Peano-Dedekind

Guiseppe Peano (1858-1932), Richard Dedekind (1831-1916)

Axiomes de Peano-Dedekind

Il existe un triplet $(\mathbb{N}, 0, s)$, où $\mathbb{N}$ est un ensemble, $0 \in \mathbb{N}$ et $s : \mathbb{N} \to \mathbb{N}$ une application appelée successeur, tel que :

(A1) s est injective ;

(A2) $(\forall n \in \mathbb{N}) \qquad s(n) \neq 0 \qquad$ (0 n'est pas un successeur : $0 \notin \mathrm{Im}(s)$) ;

(A3) axiome de récurrence (ou d'induction)

$$\left(\begin{array}{c} A \subset \mathbb{N}, \quad 0 \in A \\ x \in A \Longrightarrow s(x) \in A \end{array} \right) \Longrightarrow A = \mathbb{N}$$

• Les éléments de $\mathbb{N}$ s'appellent les entiers naturels et se notent comme l'histoire l'a imposé : 0, $1 = s(0)$, $2 = s(1)$, ...

• $\mathbb{N}$ est infini (par $(A1)$ et $(A2)$) ; son existence est affirmée ; quid de l'unicité ?

2. Sur l'unicité de $(\mathbb{N}, 0, s)$

Parmi les triplets (E, e, t), où E est un ensemble, $e \in E$, et $t : E \to E$ une application, $(\mathbb{N}, 0, s)$ se distingue par la :

propriété universelle de $(\mathbb{N}, 0, s)$

$$(PU)\begin{cases} \text{Pour tout triplet (E,e,t),} \quad \exists!\ \varphi : \mathbb{N} \to E \text{ telle que :} \\ \varphi(0) = e \quad \text{et le diagramme ci-dessous commute.} \end{cases}$$

$$\begin{array}{ccc} \mathbb{N} & \xrightarrow{s} & \mathbb{N} \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi} \\ E & \xrightarrow[t]{} & E \end{array}$$

Démonstration : Les conditions

$$\begin{cases} \varphi(0) = e \\ \forall n \in \mathbb{N}, \quad \varphi(s(n)) = t(\varphi(n)) \end{cases}$$

définissent $\varphi : \mathbb{N} \to E$ par récurrence. □

unicité de $(\mathbb{N}, 0, s)$ à bijection (unique) près

Théorème (unicité de $\mathbb{N}$)

Si (E, e, t) est un autre triplet vérifiant (PU), alors il existe une bijection et une seule $\varphi : \mathbb{N} \to E$ telle que $\varphi(0) = e$ et qui rende commutatif le diagramme :

$$\begin{array}{ccc} \mathbb{N} & \xrightarrow{s} & \mathbb{N} \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi} \\ E & \xrightarrow[t]{} & E \end{array}$$

Démonstration :

$$\begin{array}{ccc} \mathbb{N} & \xrightarrow{s} & \mathbb{N} \\ {\scriptstyle\varphi_1}\downarrow & & \downarrow{\scriptstyle\varphi_1} \\ E & \xrightarrow[t]{} & E \end{array} \qquad \begin{array}{ccc} E & \xrightarrow{t} & E \\ {\scriptstyle\varphi_2}\downarrow & & \downarrow{\scriptstyle\varphi_2} \\ \mathbb{N} & \xrightarrow[s]{} & \mathbb{N} \end{array} \qquad \begin{array}{ccc} \mathbb{N} & \xrightarrow{s} & \mathbb{N} \\ {\scriptstyle Id_{\mathbb{N}}}\downarrow & & \downarrow{\scriptstyle Id_{\mathbb{N}}} \\ \mathbb{N} & \xrightarrow[s]{} & \mathbb{N} \end{array} \qquad \begin{array}{ccc} E & \xrightarrow{t} & E \\ {\scriptstyle Id_E}\downarrow & & \downarrow{\scriptstyle Id_E} \\ E & \xrightarrow[t]{} & E \end{array}$$

□

3. Addition dans $\mathbb{N}$

Définition (addition)

$$\begin{array}{rcl} + : \mathbb{N} \times \mathbb{N} & \longrightarrow & \mathbb{N} \\ (x, y) & \longmapsto & x + y \end{array}$$

est définie (par récurrence) par

$$\left\{ \begin{array}{lrcl} (\forall x \in \mathbb{N}) & x + 0 & = & x \\ (\forall x, y \in \mathbb{N}) & x + s(y) & = & s(x + y) \end{array} \right.$$

Proposition

$(\mathbb{N}, +, 0)$ *est un monoïde, commutatif, régulier.*

Démonstration : exercice (long ...). □

4. Multiplication dans $\mathbb{N}$

Définition (multiplication)

$$\begin{array}{rcl} \cdot : \mathbb{N} \times \mathbb{N} & \longrightarrow & \mathbb{N} \\ (x, y) & \longmapsto & x \cdot y \end{array}$$

est définie (par récurrence) par

$$\begin{cases} (\forall x \in \mathbb{N}) & x \cdot 0 & = & 0 \\ (\forall x, y \in \mathbb{N}) & x \cdot s(y) & = & x \cdot y + x \end{cases}$$

Proposition

$(\mathbb{N}, \cdot, 1)$ est un monoïde, commutatif, où tout élément non nul est régulier. De plus, la multiplication est distributive par rapport à l'addition.

Démonstration : exercice (long ...). □

5. Structure d'ordre

Généralités :
Soit A un ensemble (non vide). Une relation d'ordre sur A est habituellement notée $\leq$; en terme d'ensemble, il s'agit (comme toute relation sur A) d'une partie de $A \times A$, de sorte que :

$$x \leq x' \quad \overset{\text{notation}}{\Longleftrightarrow} \quad (x, x') \in \leq \qquad (\text{étonnant non ?})$$

Définition (relation d'ordre)

Une relation $\leq \subset A \times A$ est une relation d'ordre sur A si $\leq$ est

(i) réflexive : $(\forall x \in A) \qquad x \leq x$

(ii) anti-symétrique : $(\forall x, x' \in A) \qquad \big(x \leq x' \text{ et } x' \leq x\big) \implies x' = x$

(iii) transitive : $(\forall x, x', x'' \in A) \qquad \big(x \leq x' \text{ et } x' \leq x''\big) \implies x \leq x''$

L'ordre est total si : $(\forall x, x' \in A) \qquad x \leq x' \text{ ou } x' \leq x.$
L'ordre est bon si toute partie non vide admet un plus petit élément.

Structure d'ordre sur $\mathbb{N}$

Définition ($\leq$ sur $\mathbb{N}$)

$$(\forall x, x' \in \mathbb{N}) \qquad x \leq x' \overset{\text{déf.}}{\iff} \big(\exists n \in \mathbb{N}, \quad x + n = x'\big)$$

Propriétés : (exercices)

1. 0 est plus petit élément ; $(\mathbb{N}, \leq)$ n'a pas de plus grand élément.
2. $\leq$ est un bon ordre ; en particulier, $(\mathbb{N}, \leq)$ est totalement ordonné.
3. Toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand élément.
4. $\leq$ est compatible avec l'addition :

$$(\forall x, x', n \in \mathbb{N}) \qquad x \leq x' \implies x + n \leq x' + n$$

5. $\leq$ est aussi compatible avec la multiplication.

6. Cardinaux, ensembles finis (et infinis ?)

$$\forall x, x' \in \mathbb{N}, \qquad [\![x, x']\!] \overset{\text{déf.}}{=} \{n \in \mathbb{N} \ : x \leq n \leq x'\}$$

Lemme

S'il existe une bijection $f : [\![1, n]\!] \to [\![1, n']\!]$, alors $n = n'$.

Définitions (sur les cardinaux)

1. $\mathrm{card}(A) = \mathrm{card}(B) \overset{\text{déf.}}{\iff}$ il existe une bijection $f : A \to B$.
2. $\mathrm{card}(A) = n \overset{\text{déf.}}{\iff} \mathrm{card}(A) = \mathrm{card}([\![1, n]\!])$.
   S'il existe $n \in \mathbb{N}$ tel que $\mathrm{card}(A) = n$, on dit que A est fini et possède n éléments. Sinon, on dit que A est infini.
3. On dit que A est dénombrable si A est fini ou si $\mathrm{card}(A) = \mathrm{card}(\mathbb{N})$.

$\mathbb{N}$ est infini (et dénombrable).

ensembles finis (et infinis ?)

Proposition

Soient A et B deux ensembles finis et de même cardinal, et $f : A \to B$ une application. Les trois assertions suivantes sont équivalentes :

(i) *f est injective ;*

(ii) *f est surjective ;*

(iii) *f est bijective ;*

Démonstration : par récurrence sur $n = \mathrm{card}(A)$. □

Théorème (caractérisation de l'infini)

$$A \ \ infini \iff ((\exists E \subset A, \ \ E \neq A) \qquad card(E) = card(A))$$

Démonstration : à méditer . . . □

7. Division euclidienne

Lemme ($\mathbb{N}$ est archimédien)

Soit $b \in \mathbb{N}$ *tel que* $1 \leq b$. *Alors :* $\forall x \in \mathbb{N},\ \exists n \in \mathbb{N},\quad x \leq nb.$

Démonstration : $x \leq xb$ ... □

Théorème (division euclidienne)

Soient $a, b \in \mathbb{N}$ *tel que* $b \neq 0$. *Il existe un unique couple* $(q, r) \in \mathbb{N} \times \mathbb{N}$ *tel que*

$$a = bq + r \quad et \quad 0 \leq r < b$$

Démonstration :

1. construction de $q \in \mathbb{N}$ tel que $qb \leq a < (q+1)b$;
2. existence de $r \in \mathbb{N}$ tel que $a = qb + r$ par déf. de $\leq$;
3. unicité de (b, q).

□

8. Nombres premiers selon Euclide

Vocabulaire (rappels !)

1. s'il existe $q \in \mathbb{N}$ tel que $a = qb$, on note $b|a$ et on dit que b divise a, ou que b est un diviseur de a, ou encore que a est un multiple de b.
2. Un nombre premier est un entier $p \in \mathbb{N}$, $2 \leq p$, dont les seuls diviseurs sont 1 et p. On désignera par $\mathbb{P}$ l'ensemble des nombres premiers.

Théorème (Euclide)

1. *Tout entier $n \geq 2$ qui n'est pas premier admet un diviseur $p \in \mathbb{P}$ tel que $p^2 \leq n$.*
2. *L'ensemble $\mathbb{P}$ des nombres premiers est infini.*
3. *Tout entier $n \geq 2$ admet une factorisation $n = p_1 \cdots p_k$ en nombres premiers, unique à l'ordre près.*

Démonstration : à chercher en exercice . . . □